

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-303102

(43)Date of publication of application : 14.11.1995

(51)Int.Cl.

H04L 9/00

H04L 9/10

H04L 9/12

G09C 1/00

H04K 1/00

H04N 1/44

(21)Application number : 06-095980

(71)Applicant : MITA IND CO LTD

(22)Date of filing : 10.05.1994

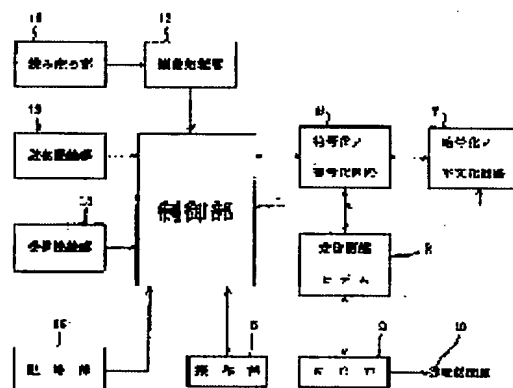
(72)Inventor : SHIBATA KOICHI

(54) COMMUNICATION EQUIPMENT

(57)Abstract:

PURPOSE: To prevent the deterioration in the security of a ciphering algorithm resulting from a fact that a head part of an original is generally at a white level by revising a CBC initial value with a prescribed arithmetic operation using number of times of communication for its factor.

CONSTITUTION: An initial setting value IV of CBC ciphering codes in 64-bits decided for each communication opposite party in the case of transmission is read from a RAM in a control section 1 comprising a microcomputer or the like. A read section 11 provided with a scanner reads a transmission original, and ciphering is applied to each block at a head of signals coded by an image processing section 12 by using the initial setting value IV. Ciphering is applied to EXOR processing between succeeding blocks and, e.g. a ciphered text of one-preceding transmission. When the communication is finished, an arithmetic operation of adding, e.g. 1 to the present initial setting value IV and the content of the RAM is rewritten. The result is used for a new initial setting value IV as an understanding with each communication opposite party.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-303102

(43) 公開日 平成7年(1995)11月14日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/00				
9/10				
9/12				
G 0 9 C 1/00		9364-5L		

H 0 4 L 9/00

Z

審査請求 未請求 請求項の数5 O L (全9頁) 最終頁に続く

(21) 出願番号 特願平6-95980

(22) 出願日 平成6年(1994)5月10日

(71) 出願人 000006150

三田工業株式会社

大阪府大阪市中央区玉造1丁目2番28号

(72) 発明者 柴田 浩一

大阪市中央区玉造1丁目2番28号 三田工業株式会社内

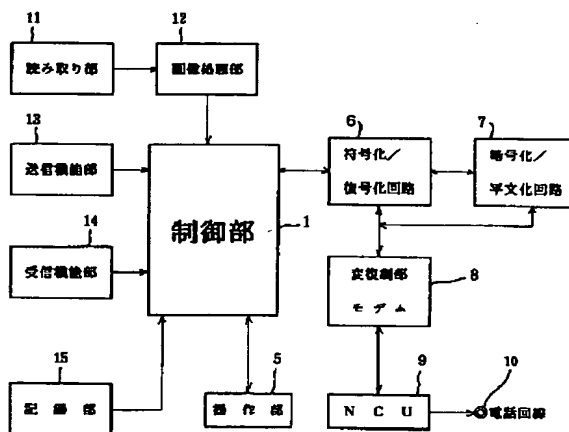
(74) 代理人 弁理士 佐野 静夫

(54) 【発明の名称】 通信機器

(57) 【要約】

【目的】 暗号アルゴリズム強度の低下を効果的に防止する。

【構成】 受信者に対するCBC初期値の初期設定を行い、CBC初期値を算術数字と考へて、送受信者間で暗号通信がなされた場合には、送信側の受信者に対するCBC初期値IVに1を加えた値に変更し、次回はその変更後の値のCBC初期値を使用するか、あるいは、暗号通信に際し、送受信者は予め取り決めたテーブルによってCBC初期値のインデックスから使用するCBC初期値を決定し、次にカウンタの値を読み出し、先に決定したCBC初期値の値とカウンタの値を加算し、その算出値をもってCBC初期値として使用することにより、暗号通信を行う毎に、自動的にCBC初期値の値を変更する。



【特許請求の範囲】

【請求項1】 C B Cモードによる暗号通信を行う通信システムの送受信モデムを構成する通信機器であって、C B C初期値を構成する数値を、通信回数を一つの要因とする演算式に基づいて通信の度に前記C B C初期値の数値データを変更し、その変更した数値データをそのときの通信時におけるC B C初期値とする機能を有する暗号通信部を具備していることを特徴とする通信機器。

【請求項2】 C B Cモードによる暗号通信を行う通信システムの送受信モデムを構成する通信機器であって、暗号通信の相手の数だけC B C初期値が必要な暗号通信機能を有する暗号通信部を備え、且つ、この暗号通信部は、前記C B C初期値を算術数値として取り扱い、暗号通信が1回終了する毎に送受信時双方とも、前記C B C初期値に所定の演算式を用いて算術演算を施し、次の暗号通信の際には、前回の暗号通信に基づき前記演算式を用いて行った数値に対応するC B C初期値を使用するように構成されていることを特徴とする通信機器。

【請求項3】 C B Cモードによる暗号通信を行う通信システムの送受信モデムを構成する通信機器であって、複数のインデックスにそれぞれC B C初期値の数値データを対応させた秘密暗号テーブルを使用する暗号通信機能を有する暗号通信部を備え、且つ、この暗号通信部は、暗号通信の相手毎に、リセット時からの通信回数を示すカウンタを有し、暗号通信実行時には、前記C B C初期値テーブルの指定されたインデックスに対応するC B C初期値の数値データに対して、前記カウンタが示す数値を加味する所定の演算式を用いて算術演算を施して、そのときのC B C初期値を設定するように構成されていることを特徴とする通信機器。

【請求項4】 C B Cモードによる暗号通信を行う通信システムの送受信モデムを構成する通信機器であって、通信回数をカウントするカウンタを有し該カウンタのカウント値をC B C初期値とする機能を有する暗号通信部を具備していることを特徴とする通信機器。

【請求項5】 ファクシミリ装置として構成された請求項1～4のいずれかの通信機器。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、暗号通信機能を有するファクシミリ装置等、秘密暗号通信を行う通信機器に係り、特に暗号通信における秘密性の向上を図った通信機器に関するものである。

【0002】

【従来の技術】ファクシミリ通信では同一メーカーのファクシミリ装置間での通信に関しては、オプションとして種々の特殊通信を行うことができる。その特殊通信の一つに暗号通信がある。

【0003】図7はファクシミリ装置における通常の暗号通信の手順を示している。図7(A)において、91

～94は送信側での信号処理手順であって、送信しようとする原稿は、まず、スキャナ91によって読み取られる。読み取られた画像データは92でMH等のデータ圧縮、つまり符号化処理される。次いで、この圧縮された画像データに対して秘密通信とすべく、93で秘密暗号鍵を用いて暗号化処理が施され、その暗号化データが送信側モデム94としてのファクシミリ装置から送出される。

【0004】このように従来では、ファクシミリ装置を用いて暗号通信を行う際には、スキャナ91で読み取った画像データを、そのまま加工を施すことなく、スキャナ91で読み取った順序に従って暗号化して送信していた。

【0005】図7(B)において、95～98は受信側での信号処理手順であって、受信側モデム95としてのファクシミリ装置で受信された原稿の暗号受信データは96で送信側と同一の秘密暗号鍵を用いて暗号文を解読する、いわゆる平文化処理が施される。平文化された画像データは97でデータ伸長、つまり復号化され、元の画像データとなり、プリンタ98により印刷され、これによって受信側で原稿が取り出される。なお、ここで言う秘密暗号鍵は一種のデータである。

【0006】図8は典型的な送信原稿の一例を示している。なお、図示例の原稿はC C I T T (国際電信電話諮問委員会)の標準原稿である。さて、この原稿Mから明らかなように、通常の送信原稿は殆どの部分が“白”つまり文字等が書き込まれていない白地部分で占められている。

【0007】いま、従来のファクシミリ装置において、スキャナ91により最初にスキャンされる部分、言い換えれば送信データの最初の部分または、最初に暗号化される部分について考えると、原稿Mで最初にスキャンされるのは、その先頭部分Hである。通常この先頭部分Hは全白であることが多い。このような理由により従来のファクシミリ装置で何らかの原稿を送出しようとする場合は、その送出データの最初の部分は全白に対するデータに対応する可能性が非常に高いと言える。

【0008】図9はファクシミリ装置における一般的な暗号化処理部の一例として、(A)はE C Bモードを用いた例を、また、(B)はC B Cモードを用いた例をそれぞれ示している。図9(A)(B)に示したいずれの場合も、通常は前述のように、平文Pに対して秘密暗号鍵Kを用いて暗号文Cを出力する。

【0009】但し、E C Bモードでは図9(A)に示すように、暗号を掛けようとする画像データと暗号が1:1で対応している。これに対し、C B Cモードでは図9(B)に示すように、例えばn番目の平文P_nを暗号化する際、その1回前の暗号文C_{n-1}と平文P_nとのE O R (排他的論理和)を取り、その結果を暗号化する。なお、この場合、1番目の画像データは暗号文が書かれて

いないため、予め秘密に設定された初期値を用い、この初期値と平文 P_1 とのEORを取ることになる。

【0010】

【発明が解決しようとする課題】このように暗号通信を行う場合、通常、人目に触れるのは暗号文Cのみであるので、その暗号が解読される可能性は可成り低いと言える。しかしながら、送信データの最初のスキャン部分は前述のように“全白”に対するデータであることが多い。このため、画像データと暗号が1:1で対応しているECBモードによるものでは、スキャナ91で原稿Mを読み取らせるとき、受信された暗号化データの始めの部分は“白”を暗号化したものであることが分かってしまい、暗号化アルゴリズムの強度に欠ける。

【0011】また、CBCモードでは、初期値は既知ではないため、1番目の画像データが“白”であっても、この“白”を表す平文 P_1 にもスクランブルが掛けられているため、ECBモードの場合よりも暗号化アルゴリズムの強度は高いと言えるが、送出データの最初の部分は“白”である点はECBモードの場合と異なるものではなく、したがって、いずれのモードにおいても、平文P(全白のデータ)と、それに対する暗号文Cが公開されているようなものである。このように従来装置の場合、特定の平文とそれに対する暗号文が既知になるので、この暗号の強度は可成り低下するという問題点があった。

【0012】本発明は、上記のような問題点に鑑みてなされたもので、CBCモードによる暗号通信を行う通信システムの送受信モデムを構成する通信機器において、通常原稿の先頭部分が殆どの場合“全白”であること等による暗号アルゴリズム強度の低下を防止するための効果的な対策を施した構成とすることを目的とするものである。

【0013】

【課題を解決するための手段】上記目的を達成するために本発明では、CBC初期値を構成する数値を、通信回数を一つの要因とする演算式に基づいて通信の度に前記CBC初期値の数値データを変更し、その変更した数値データをそのときの通信時におけるCBC初期値とする機能を有する暗号通信部を具備するものとしている。

【0014】暗号通信部の具体的構成としては、第1に、暗号通信の相手の数だけCBC初期値が必要な暗号通信機能を有し、且つ、前記CBC初期値を算術数字として取り扱い、暗号通信が1回終了する毎に送受信時双方とも、前記CBC初期値に所定の演算式を用いて算術演算を施し、次の暗号通信の際には、前回の暗号通信に基づき前記演算式を用いて行った数値に対応するCBC初期値を使用するものとしている。

【0015】また、第2の構成としては、複数のインデックスにそれぞれCBC初期値の数値データを対応させたCBC初期値テーブルを使用する暗号通信機能を有し、且つ、暗号通信の相手毎に、リセット時からの通信

回数を示すカウンタを有し、暗号通信実行時には、前記秘密暗号テーブルの指定されたインデックスに対応するCBC初期値の数値データに対して、前記カウンタが示す数値を加味する所定の演算式を用いて算術演算を施して、そのときのCBC初期値を設定するものとしている。尚、カウンタのカウント値をそのままCBC初期値とする構成も可能である。

【0016】

【作用】上記構成によると、受信者に対するCBC初期値の初期設定を行い、CBC初期値を算術数字と考えて、送受信者間で暗号通信がなされた場合には、送信側の受信者に対するCBC初期値を例えば予め取り決めた値を加算する等の演算を行って変更し、次回はその変更後の値のCBC初期値を使用する。以下同様に、暗号通信を行う毎に、演算を行う。受信側も同様に、送信者から暗号通信を受信する度に、送信者に対するCBC初期値を変更する演算を行う。

【0017】また、CBC初期値テーブルを利用するものでは、暗号通信に際し、送信側はユーザーに設定されたCBC初期値のインデックスにより、使用するCBC初期値を決定し、次に、カウンタの値を読み出し、先に決定したCBC初期値の値とカウンタの値を例えば加算するような算術演算を行う。そして、暗号通信にはその演算によって得られた値をCBC初期値として使用する。受信側も同様な処理を行う。

【0018】

【実施例】以下、本発明の実施例を図面を参照しながら説明する。CBCモードによる暗号通信を行う通信システムの送受信モデムを構成するファクシミリ装置に適用した実施例を図面を参照しながら説明する。図1は本発明の第1実施例に係るファクシミリ装置の全体構成をブロック図で示している。

【0019】この図において、1はマイクロコンピュータ等からなる制御部であって、全体の制御を司る。この制御部1は図2に示すように、CPU2、プログラムROM3、RAM4等から構成されている。また、RAM4は暗号通信を行うときのワーク領域、メモリ領域の一つの形態としての暗号鍵記憶領域、CBC初期値(1V)記憶領域、カウンタ等を有している。

【0020】図1に戻って、5は操作部、6は符号化/復号化回路、7は当該ファクシミリ装置が送信側として動作するときは、暗号化を行い、受信側として動作するときは平文化を行う暗号化/平文化回路、8は変復調部モデム、9はNCU(網制御装置)、10は公衆電話回線である。11は原稿を読み取るスキャナ11aを有する読み取り部である。12は読み取った画像データにシェーディング補正等の処理を施す画像処理部である。13は送信機能部、14は受信機能部、15はプリント部15a等を有する記録部である。

【0021】上述した操作部5、変復調部モデム8及び

NCU9、スキヤナ11a、プリント部15a、リアルタイムクロック16とCPU2とは図2に示すように、データバス16を通して接続されており、CPU2を中心とする上記各構成は、以下に述べるように、原稿を正方向及び逆方向で暗号化する暗号通信部として機能するものであり、送受信双方とも、暗号通信としてのプロセスが制御部1においてプログラムされている。

【0022】次に、上記構成が暗号通信部として機能する場合について、送信側として動作するときの制御部1の動作例を図3のフローチャートを参照しながら説明する。本実施例ではCBCモードの初期値を使用して、秘密暗号鍵を通信毎に変化させる方法を示す。この場合、CBCモードを利用しているため、先頭のブロック(ここでは64ビット)のみ全白対応をすればよい。すなわち、CBC初期値は通常、64ビット程度の2進数の数値データである。

【0023】まず、暗号通信を行う送受信者は共に本実施例装置を使用しているものとする。本実施例では送信者が暗号通信しようとする相手に対し、各々の相手固有のCBC初期値が存在するような方式を考える。したがって、この場合、暗号通信しようとする相手の数だけCBC初期値が存在することになる。

【0024】図3において、送信者が送信動作を開始し、ステップ#105で通信相手に対応するCBC初期値IVをRAM4のCBC初期値記憶領域から読み出す。ここでは、受信者に対するCBC初期値をIVとする。なお、この初期設定値IVは前述のとおり64ビットの2進数であり、例えば“0000000000000000”等の形で表される。次いで、ステップ#110で、スキヤナ11aで読み取られた送信原稿を符号化し、さらにステップ#115で、符号化された原稿を前記CBC初期値IVにより暗号化する等の通信手順が行われ、ステップ#120で最終的に送信動作が行われる。

【0025】送信後は、CBC初期値IVの変更が行われる。本実施例では、CBC初期値の数値データを算術数字として取り扱う。そして、暗号通信が1回終了する毎に、CBC初期値に所定の演算式を用いて算術演算を施し、次の暗号通信の際には、前回の暗号通信に基づき前記演算式を用いて行った数値に対応するCBC初期値を使用する。この演算式は、 $IV' = IV + 1$ で表される。

【0026】したがって、送受信者間で暗号通信がなされた後は、ステップ#125で送信側の受信者に対するCBC初期値を“IV”から“IV+1”に変更し、次回はこの“IV+1”を特定の相手に対するCBC初期値として使用するべく、ステップ#130で新たにIV'をCBC初期値としてRAMのCBC初期値記憶領域に格納する。

【0027】以下同様に、暗号通信を行う毎に、CBC

初期値の値に“1”を足し算する。受信側も同様に、送信者から暗号通信を受信する度、送信者に対するCBC初期値に“1”を足す。なお、本実施例では、例題としてCBC初期値に“1”を足す演算を示したが、他の数式による算術演算を用いるようにしてもよい。

【0028】図4は本実施例装置が受信側として動作するときの制御部1の動作例を示している。受信側においては、受信後、ステップ#205で通信相手に対応するCBC初期値IVをRAM4のCBC初期値記憶領域から読み出す。次いで、ステップ#210で受信データを一旦、RAM4へ格納する等の所定手順の受信動作を行った後、ステップ#215で先に読み出したCBC初期値IVで受信原稿の平文化を行い、さらにステップ#220でそれを復号化し、受信を完了する。

【0029】この後、受信側においても、ステップ#225で送信側の受信者に対するCBC初期値を“IV”から“IV+1”に変更し、次回はこの“IV+1”を特定の相手に対するCBC初期値として使用するべく、ステップ#230で新たにIV'をCBC初期値としてRAMのCBC初期値記憶領域に格納する。

【0030】このように本発明の第1実施例では、暗号通信が1回終了する毎に送受信時双方とも、CBC初期値に所定の演算式を用いて算術演算を施し、次の暗号通信の際には、前回の暗号通信に基づき前記演算式を用いて行った数値に対応するCBC初期値を使用するものであるため、CBC初期値を暗号通信しようとする相手の数だけ登録すれば、通信の相手毎に秘密暗号鍵を変更することが可能になるため、暗号強度アップの点で有利であると言える。

【0031】図5及び図6は、本発明の第2実施例における制御部1の送信動作(図5)と、受信動作(図6)の流れを示している。なお、本実施例の構成は、図1及び図2に示した上記第1実施例のそれと共通しているため、共通の構成についてはその説明を省略する。

【0032】本実施例においては、送信者が暗号通信しようとする相手に対し、下記表1に示すようなRAM4のCBC初期値テーブルを使用する。このCBC初期値テーブルは、CBC初期値を適宜数登録し、それぞれのCBC初期値としての数値データ毎にインデックスを施したものであって、実際の使用に際しては、CBC初期値そのものではなく、インデックスを用いる。したがって、暗号通信の相手の数だけCBC初期値が存在するわけではなく、相手によっては、他の相手と同じCBC初期値を使用する可能性もある。なお、該CBC初期値テーブルは機器製造時において、ユーザーに対して予め設定しておくものとする。

【0033】

【表1】

10

20

30

40

インデックス	CBC初期値
00	0000000000000000
01	0123456789ABCDEF
02	2222222222222222
03	FEDCBA9876543210
04	1111122222333335
05	1122334455667788

【0034】また、送受信双方の制御部1には暗号通信の相手毎に、リセット時からの特定の送受信者間の通信回数を示すカウンタがソフト的に設けられている。なお、実際には、暗号通信する相手の数だけ、このカウンタが必要になる。いま、このカウンタが示す値を“C”とする。

【0035】そして、暗号通信に際し、送信側は図5に示すように、暗号通信を実行するために送信を開始した後、ステップ#305でCBC初期値テーブルから指定されたインデックスを読み出し、使用するCBC初期値を決定する。この場合、表1を参照して、例えばインデックスが“05”と指定されているとすると、“1122334455667788”を選択することになる。いま、このCBC初期値の値を“IV”とする。

【0036】次いで、ステップ#310で通信相手に対応したカウンタの値Cを読み出す。この送信に際しては、CBC初期値IVの変更が行われる。本実施例においても、CBC初期値の数値データを算術数字として取り扱う。すなわち、指定されたインデックスに対応するCBC初期値の値IVに対して、カウンタが示す数値Cを加味する所定の演算式を用いて算術演算を施し、その算出値IV'をそのときのCBC初期値の値とする。この演算式は、 $IV' = IV + C$ で表される。したがって、例えば特定の相手との通信回数が10回目であるとすれば、カウンタの値Cが10であるから、そのときの送受信者双方のCBC初期値の値IV'は“1122334455667798”となる。

【0037】次いで、ステップ#315で送信画像（原稿）の符号化を行い、ステップ#320で所定手順で送信動作を行う。このとき暗号通信には前記“IV+C”をCBC初期値として使用する。なお、本実施例においても、CBC初期値を決定する算術演算は上記とは異なる数式を用いるようにしてもよい。

【0038】そして、送信後、ステップ#325で暗号通信が1回終了する毎に、使用したカウンタの値に1を足し算し、ステップ#330でこれによって得られた値C'（C+1）を、RAM4のCBC初期値記憶領域に格納しておく。次回の暗号通信の際には、改めてCBC初期値テーブルから指定したインデックスを読み出し、使用するCBC初期値を決定するとともに、カウンタの値としてC'を用いることになる。このため、例えば続けて同じインデックスを指定したとしても、CBC初期値のデータは異なる値となるので、秘密暗号鍵の暗号強度が低下することはない。

【0039】図6は本実施例装置が受信側として動作するときの制御部1の動作例を示している。受信側においては、受信後、ステップ#405で通信相手と対応するCBC初期値テーブルのインデックスを読み出し、使用するCBC初期値を決定し、次いで、ステップ#410で通信相手に対応したカウンタの値Cを読み出す。そして、送信側と同じCBC初期値、すなわち“IV+C”を暗号鍵として受信データの平文化を行い、ステップ#420で受信原稿の復号化を行い、受信を完了する。

【0040】この後、受信側においても、ステップ#425で送信側の受信者に対するカウンタの値を“C”から“C+1”に変更し、ステップ#430で得られた値C'（C+1）をRAM4のCBC初期値記憶領域に格納する。

【0041】このように本発明の第2実施例では、暗号通信実行時には予め設定された秘密暗号テーブルの指定されたインデックスに対応するCBC初期値の数値データに対して、カウンタが示す数値を加味する所定の演算式を用いて算術演算を施すことにより、そのときのCBC初期値を設定するようにしており、CBC初期値を相手の数だけ準備しなくてもよいので、暗号通信を前記第1実施例よりも簡単に行うことができる。

【0042】次に、本発明の第3の実施例は、CBC初期値として通信回数をカウントするカウンタの値を、そのまま使う。送信側と受信側のカウンタは通信回数をカウントする。そのカウント値は前記CBC初期値IVとして使用される。この第3実施例では、カウンタの値をそのまま初期値として使用するの、他に初期値を用意しておいたり、算術演算を施したりする必要がないというメリットがある。

【0043】

【発明の効果】以上説明したように本発明によるときは、CBC初期値を構成する数値を、通信回数を一つの要因とする演算式に基づいて通信の度に前記CBC初期値の数値データを変更し、その変更した数値データをそのときの通信時におけるCBC初期値とする機能を有するものとしているので、CBCモードによる暗号通信を行う場合、送信データ量を全く変化させず送信することができるものでありながら、平文と暗号文のペアが既知とならず、暗号の強度が低下することがない。

【0044】すなわち、本発明では、秘密暗号鍵の変更のために必要な演算を機器が自動的にを行い、且つ、その演算結果に基づきCBC初期値のデータを自動的に変更していくので、ユーザーは簡単な操作でもって高度な暗号強度を有する暗号通信を実現することができる。

【0045】また、暗号通信部の具体的構成として、請求項2ではCBC初期値を算術数字として取り扱い、暗号通信が1回終了する毎に送受信時双方とも、前記CBC初期値に所定の演算式を用いて算術演算を施し、次の暗号通信の際には、前回の暗号通信に基づき前記演算式を用いて行った数値に対応するCBC初期値を使用するものとしているので、CBC初期値を暗号通信しようとする相手の数だけ登録すれば、通信の相手毎にCBC初期値を変更することが可能になるため、暗号強度アップの点で有利なものとなる。

【0046】さらに、請求項3では暗号通信の相手毎にリセット時からの通信回数を示すカウンタを有し、暗号通信実行時には、前記秘密暗号テーブルの指定されたインデックスに対応するCBC初期値の数値データに対して、前記カウンタが示す数値を加味する所定の演算式を用いて算術演算を施して、そのときのCBC初期値を設定するものとしているので、CBC初期値を相手の数だけ準備しなくてもよく、したがって暗号通信を請求項2のものよりも更に簡単に行うことができる。

【0047】また、請求項4では、CBC初期値として通信回数をカウントするカウンタの値をそのまま初期値として使用するの、他に初期値を用意しておいたり、

算術演算を施したりする必要がない。

【0048】そのうえ、上記したいずれの構成においても、例えばエラーの発生等により同じ原稿が繰り返し送信されることがあっても、先頭の画像データはその送信時毎に異なるので、暗号強度が一層高まり、例えば通常原稿の先頭部分が殆どの場合“全白”であることによる暗号アルゴリズム強度の低下を効果的に防止することができる。

【図面の簡単な説明】

【図1】 本発明の第1実施例に係るファクシミリ装置の構成を示す概略ブロック図。

【図2】 その制御部を具体的にするとともに他の構成部分との接続状態を示すブロック図。

【図3】 制御部の送信に関する動作例を示すフローチャート。

【図4】 同制御部の受信に関する動作例を示すフローチャート。

【図5】 本発明の第2実施例に係るファクシミリ装置における制御部の送信に関する動作例を示すフローチャート。

【図6】 同制御部の受信に関する動作例を示すフローチャート。

【図7】 一般的なファクシミリ装置における通常の暗号送信の手順を示すブロック図。

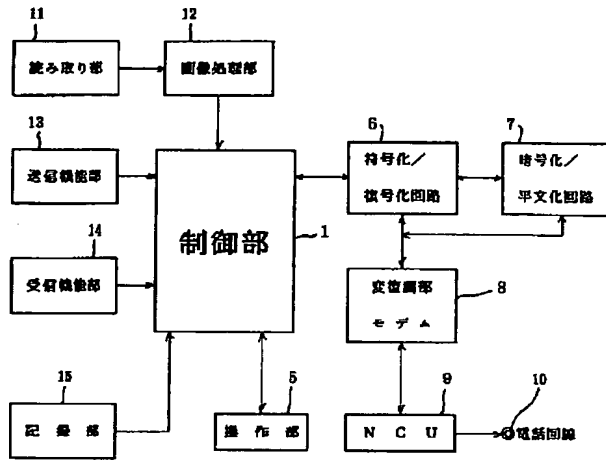
【図8】 送信原稿の一例を示す平面図。

【図9】 一般的なファクシミリ装置における暗号化処理部の一例を示すブロック図。

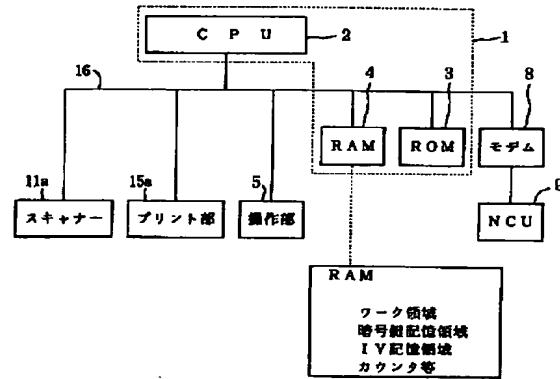
【符号の説明】

- 1 制御部
- 2 CPU
- 3 ROM
- 4 RAM
- 5 操作部
- 6 符号化／復号化回路
- 7 暗号化／平文化回路
- 8 変復調部モデム
- 9 NCU
- 11 読み取り部
- 11a スキャナ
- 12 画像処理部
- 13 送信機能部
- 14 受信機能部
- 15 記録部
- 15a プリント部

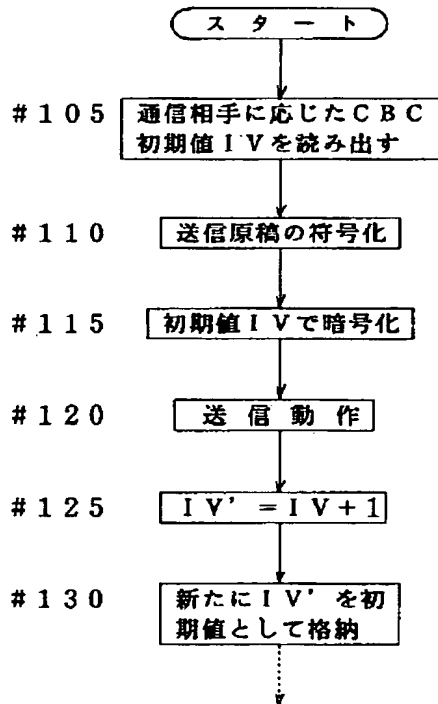
【図1】



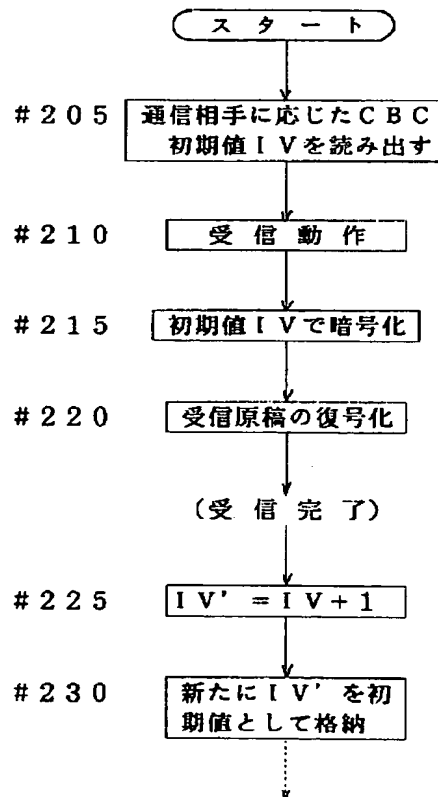
【図2】



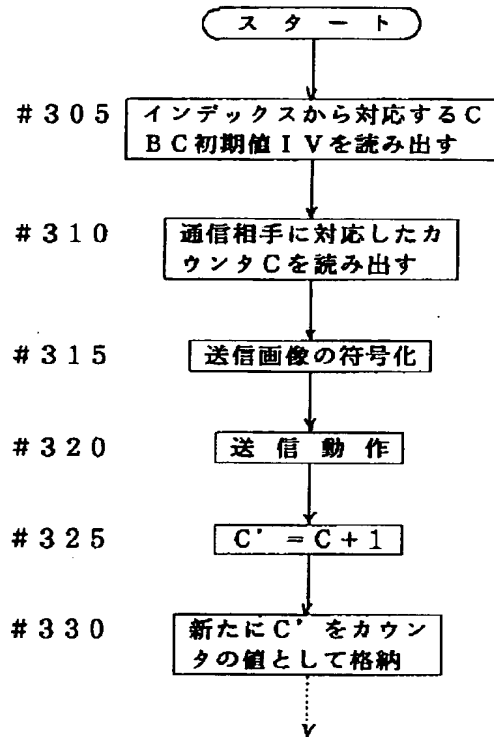
【図3】



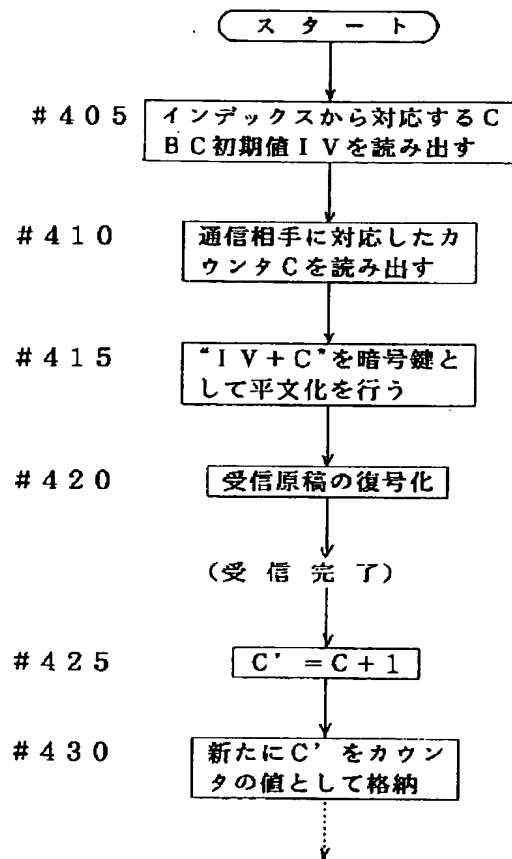
【図4】



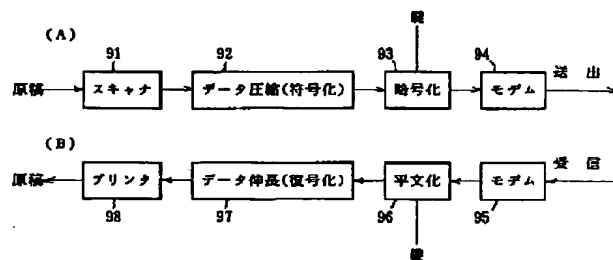
【図5】



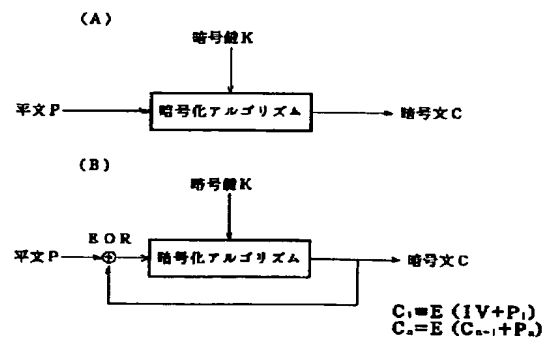
【図6】



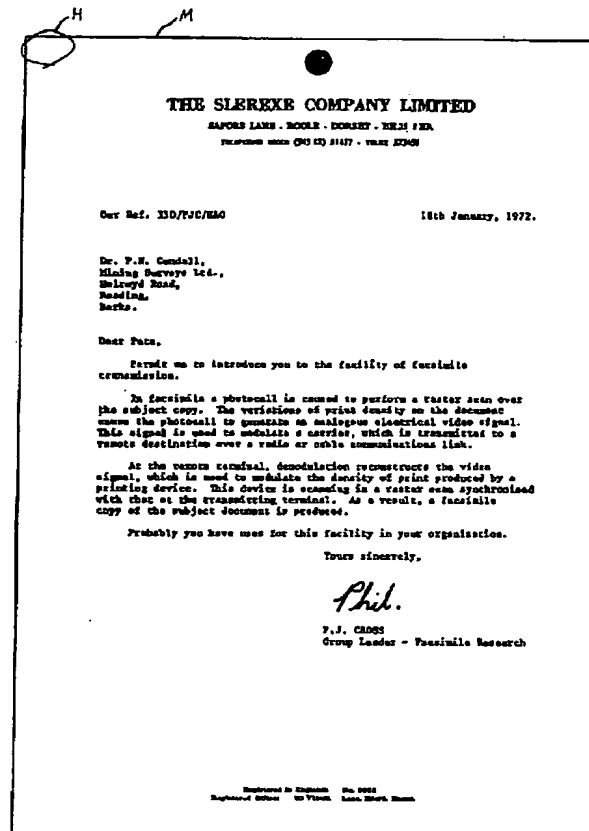
【図7】



【図9】



【図8】



フロントページの続き

(51)Int.Cl.⁶

H 0 4 K 1/00

H 0 4 N 1/44

識別記号

庁内整理番号

F I

技術表示箇所

Z